TECHNICAL DOCUMENT 3277
February 2019

TIPPERS Evaluation at SSC Pacific

Dr. Mamadou H. Diallo

Christopher T. Graves

Approved for public release.

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

M. K. Yokoyama, CAPT, USN
Commanding Officer

W. R. Bonwit
Executive Director

ADMINISTRATIVE INFORMATION

The work described in this report was performed for DARPA Brandeis Program by the PAC 58200 Branch (58240) of the Cybersecurity Engineering Division (Code 58), Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA.

Released by
Vic Beach, Head
PAC 5840 Branch

Under authority of
Jara D. Tripiano, Head
Cybersecurity Engineering Division

The citation of trade names and names of names of manufacturers is not to be construed as official government endorsement or approval of commercial products or services referenced in this report.

Rasp Pi™ software is a registered trademark of Raspberry Pi Foundation

IoT™ is a registered of trademark of IBM

TIPPERS contact information: http://tippersweb.ics.uci.edu/

CONTENTS

Figures

This page intentionally left blank.

1. PROJECT: TIPPERS EVALUATION AT SSC PACIFIC

1.1 OVERVIEW

This technical document details our effort in deploying and evaluating TIPPERS (Testbed for IoT-based Privacy-Preserving PERvasive Spaces) at the Space and Naval Warfare Systems Center Pacific (SSC Pacific). TIPPERS is an Internet of Things (IoT™) testbed being developed at the University of California, Irvine (UCI) by a number of performers, under the DARPA's Brandeis program (https://www.darpa.mil/program/brandeis). TIPPERS takes care of capturing data from IoT devices (e.g., beacons, Wi-Fi access points, video cameras, microphones), abstracting such data into higher-level semantic interpretations, and offering these abstractions to developers to build smart applications. TIPPERS follows a ***privacy-by-design*** approach and incorporates different cryptographic based privacy and security technologies. In TIPPERS, the different phases of data management (capture, storage, sharing, abstraction) are regulated by policies.

1.1.1 TIPPERS POLICY MODEL

The TIPPERS policy model is supported on multiple facets such as policy specification, enforcement, and attestation. In addition, the high-level policies are translated into lower device level policies to bridge the semantic gap at application layer. It also provides integration platform for various privacy technologies. Currently, it is customized as a system to manage smart spaces and is deployed at the Donald School of Information and Computer Sciences at UCI.

This page intentionally left blank.

2. EVALUATION PHASES

2.1 TWO PHASE APPROACH

The evaluation effort is divided into two phases.

- **Phase 1**: Integration of TIPPERS into two lab environments at SSC Pacific, MobileLand and NACS (Navy Advanced Cyber Security) labs, to evaluate its features and performance, and
- **Phase 2**: Development of scenarios for potential use of TIPPERS as a Navy ashore or afloat system.

This document focuses on Phase 1.

During the first phase of the project, our team plans on deploying TIPPERS in the MobileLand lab environment and evaluate its features. The following section describes the envisioned use cases for deploying and evaluating TIPPERS.

2.2 USE CASES

Our team uses the following three use cases to analyze TIPPERS:

1. **Device Management and Monitoring:** monitoring and report the health status of all connected devices.
2. **Location-based resource management:** providing access to resources including files based on the locations of the users.
3. **Visitor tracking:** automate visitors escorting in Navy bases.

2.3 ACTORS

- **Visitors**: Visitors to SSC Pacific.
- **Hosts:** SSC Pacific employees who can escort visitors at the center.
- **TIPPERS Administrators**: SSC Pacific employees who manage TIPPERS.

2.4 ASSUMPTIONS

There are two assumptions that we make in evaluating TIPPERS:

- We assume that the TIPPERS system has been deployed in MobileLand, and all the IoT™ devices in MobileLand have been configured and registered into the system.
- We assume that there are two types of badges, white badges for employees and red badges for visitors. When an employee is escorting a visitor, he or she, needs to carry a tracking device (for example, a smart phone) to track the visitor. The tracking device tracks the distance between the visitor and the escort, using a beacon attached to the red badge and connected to the phone carried by the escort, see Figure 1.

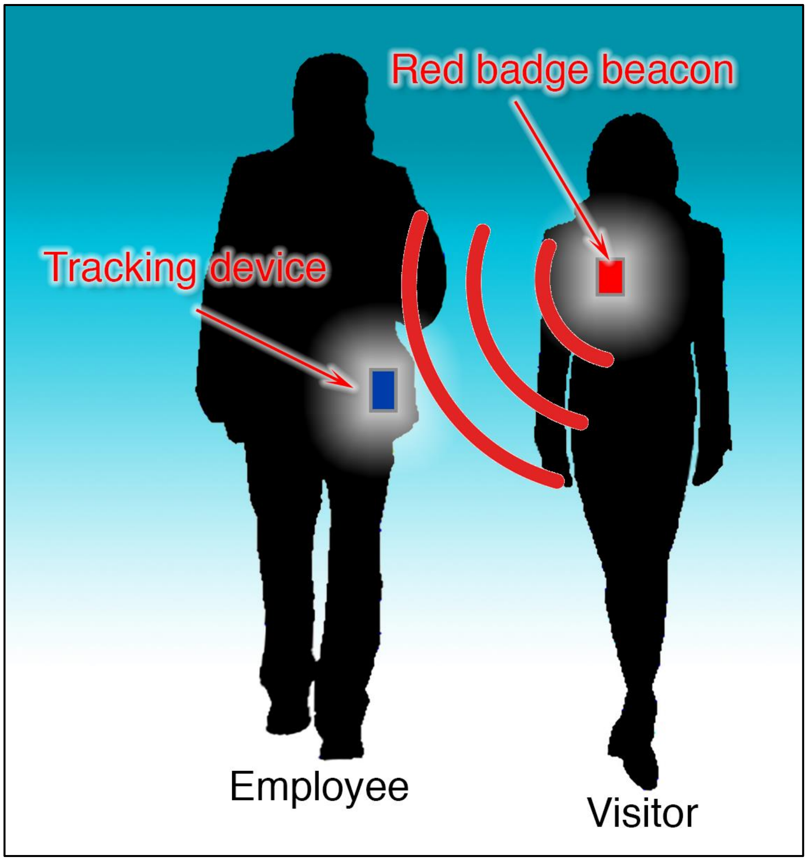

Figure 1. TIPPER badge tracker.

2.5 PRIVACY POLICIES

Privacy policies are as follows:

- P1: A visitor should not be away from the host more than x feet. **[Surveillance Policy]**
- P2: The precise location of a visitor and a host is shown on the TIPPERS dashboard only if P1 is violated. **[Privacy policy]**
- P3: The TIPPERS Administrator cannot see the exact location of the visitor and host, only estimated location (ex. Computed using differential privacy). **[Privacy policy]**

3. APPLICATIONS DESCRIPTION

3.1 OVERVIEW

This section details three subsets of Applications that are covered in this Section: Visitor Tracking System, Device Management and Monitoring and Location Based Resource Management shown in Figure 2.

Visitor Tracking System
Device Management and Monitoring
Location based Resource Management

Figure 2. Three subsets of Applications.

3.1.1 Visitor Tracking System:

Currently, visitors tracking at SSC Pacific is done manually. An employee must always escort a visitor and prevents the visitor from illegal activities including going into restricted areas. An advanced tracking system would address the problem of false-negatives that occur due to human errors. The tracking systems would provide accountability when false-positives are found. The system would do this by utilizing a smart sensing capability through interconnected sensors such that actors (visitors and escorts, Figure 1) are constantly kept under surveillance.

3.1.1.1 Requirements:

- **Robustness**: from a systems perspective,
  - ✓ (a) secure storage: no identifiable/correlate-able piece of data/information should be publicly available,
  - ✓ (b) secure distribution: no sensitive information should be handed without any secure masking methods.
- **Privacy**: The privacy policies allow that visitor tracking system stays *anonymous* unless a warning is generated that the visitor is farther than x feet away from the escort. In this case, the privacy is not obeyed and the actual location is revealed/displayed on the dashboard.

3.1.2 Device Management and Monitoring:

Currently, there is no device management and monitoring system for IoT devices at SSC Pacific. Such a system can be used for various tasks in IoT based systems including assessing the device states in real-time, pushing security policies into the devices dynamically when applicable, and automatic scanning the devices for vulnerabilities. The system would provide collective ping to an authentic set of registered devices. For example, all set of devices are required to switch the on/off mode at the same time. In this case, a single command from the admin system can collectively actuate the set of devices with the concerned policy. In addition, any foreign devices should be detected and verified regarding the policy adherence. The primary actors would be administrator, devices and device owners (if any).

3.1.2.1 Requirements:

- **Robustness**: from a systems perspective,
  - ✓ (a) Reliability: No lesser and no more devices but only the required set of devices be triggered for any kind of actions.
  - ✓ (b) Recoverability: Device anomalies should be identified at the earliest possible time.
- **Privacy**: The privacy policies allow that the device status (online, offline, ideal, upgrading) or the transition from one state to another to be done subliminally such that there is no obvious pattern to device handling norms.

3.1.3 Location based Resource Management:

Currently, the location based resource management is enforced through physical barriers such as card swipe entrance, biometric credential identification, etc. An advanced system would enable the resource access more seamless and secure (imagine if a card is stolen then the whole place is fully accessible). The primary actors would be set of sensitive resources, users requesting access, and a validation system to decide the scope (What level is it available in? How long is it available for? Can one know about the possible inconsistencies due to many users accessing the same resource at same location, simultaneously?) of accessibility.

3.1.3.1 Requirements:

- **Robustness**: from a systems perspective,
  - ✓ (a) Consistency: multiple users accessing the resources at the same time and same place.
  - ✓ (b) Data handover: devices must leave/erase all sensitive information before leaving the current location.
- **Privacy**: The privacy policies allow that resources are non-shareable and non-forwardable beyond the restricted access zone. In addition, any trails of a sensitive data currently being accessed is securely removed from the devices before the device migrates to a different location possibly with a different privacy policy.

4. TIPPERS DEPLOYMENT

4.1 OVERVIEW

MobileLand is a lab dedicated for testing and evaluating mobile technologies. The lab is divided into five areas: meeting, visitors, offices, machines, and kitchen. The lab has its own wireless network. The TIPPERS core system will be deployed in MobileLand in a dedicated server.

The following three selected applications will be deployed on top of the core system: Device Management and Monitoring, Location-based Resource Management, and Visitor Tracking.

The following types of devices will be used to realize the applications: Wi-Fi access point, smart phone, camera, beacon, and Raspberry Pi.

Figure 3 shows the MobileLand floor plan for the TIPPERS deployment. We divide the floor into four zones based on the lab space utilization. In each zone, the locations where the IoT devices will be deployed are shown. This zoning enables the definition of granular policies.

Sample Implementation: It would require Wi-Fi routers (with Rasp Pi™ software), Bluetooth beacons, camera, user devices like cellphones and other smart wearables, system server (i5 or i7) with 1 TB storage, approximately.

Privacy Technologies Used: The privacy is ingrained in TIPPERS system right from the raw data collection (e.g., MAC addresses used as a digest) to data sharing based on policy preferences, and from policy attestation (e.g., through secure sensor data access) to Differentially private observation/analysis of the raw data. Policy model provides a tool for privacy regulation at fine-grained level, e.g., individuals may identify and restrict access to a specific group of people to every information related to them.

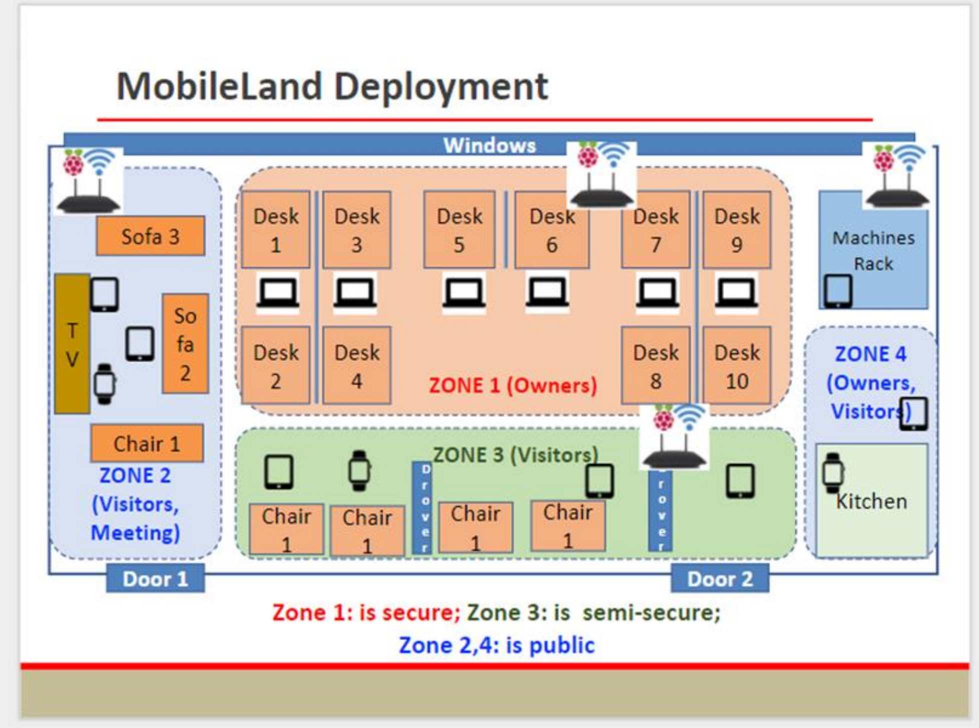

Figure 3. The MobileLand floor plan for the TIPPERS deployment.

This page intentionally left blank.

5. DEMONSTRATION DELICIOUS

5.1 OVERVIEW

This section contains a demo that is comprised of supporting three scenarios:

1. **Surveillance**: Demonstration of the monitoring of the distance between the Escort and Visitor.
2. **Privacy Enforcement**: Demonstration of the privacy preservation of the location of the Escort and Visitor toward the Admin user, but not the Manager.
3. **Policy Violation**: Demonstration of the alert when the distance policy between the Escort and visitor is violated.

5.2 DEMO SCRIPT

This section applies the three scenarios of Surveillance, Privacy Enforcement, and Policy Violation in a demonstration script format.

In his scenario Alice is the Visitor to MobileLand and John is the host, see Figure 4 setup for this demonstration is shown in Figure 1.

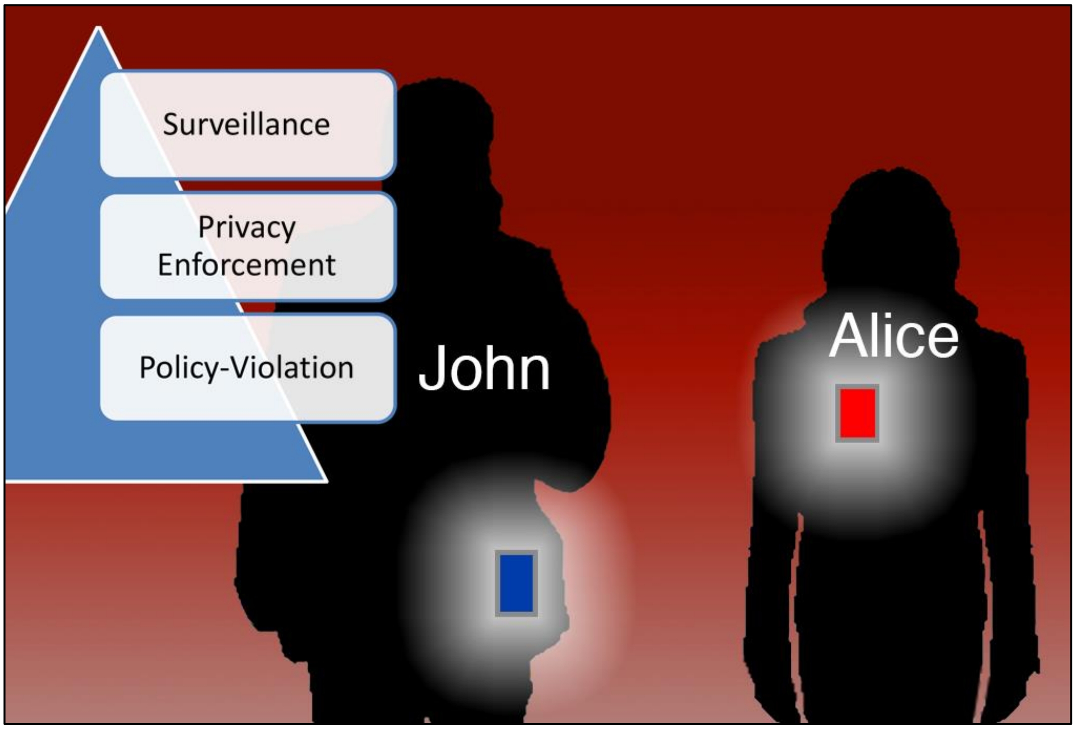

Figure 4. The Demonstration Script applies three criteria's.

The demonstration script is as follows:

1. John, before picking up Alice from the Gate, launches the TIPPERS Visitor Tracking application on his phone.
2. Previously John setup the Visitor Tracking application to hone into the beacon attached to the red badge reserved for Alice.
3. After meeting with Alice at the Gate, John gives the red badge to Alice and informs her that the badge is equipped with a tracking device.
4. John and Alice walk toward MobileLand. When they arrive in the corridor, the TIPPERS system automatically detects that John's phone is tracking Alice's red badge.
5. TIPPERS starts monitoring the distance between John and Alice. TIPPERS continuously records the locations of John and Alice.
6. TIPPERS presents two views of the locations information.
    a. In the Management View, TIPPERS continuously displays the precise locations of John and Alice.
    b. In the Admin View, TIPPERS shows only approximate locations information.
7. Alice steps out of MobileLand but John stays inside the room.
8. As Alice is moving away from John, the Admin Dashboard shows the distance between John and Alice is increasing.
9. After the distance between the two reaches 5 feet, the Admin Dashboard rings an alarm.
10. The Admin Dashboard then shows the precise location of the John and Alice.

6. LESSONS LEARNED

In Our team research using TIPPERS has shown it has many advantages over the current visitor scenario. These include:

- It is possible to track more than one person at a time
- Custom alarms can be set if the tracked person is further away from the host then a set distance.
- External personnel are able to view the host and tracked person through a separate monitor.
- Global positioning allows the tracked person to be positioned on a site map so their location is known at all times.

6.1 FUTURE RESEARCH

- Although not available currently, research is being done on a tracking device that can be attached to a person with a special adhesive that is not removable for a period of two hours, or can be removed with a special developed solution that makes it possible to remove the patch before two hours.
- Research is being done on a special phone application that can be loaded on the visitor cell phone, this application will make it so that the phone generates a tracking signal so that the phone may be tracked. The only way this application can be removed is by entering a special password.

This page is intentionally left blank.

INITIAL DISTRIBUTION

84300	Library	(1)
85300	Archive/Stock	(1)
58240	M. Diallo	(1)
58240	C. T. Graves	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
February 2019	Final	

4. TITLE AND SUBTITLE

Tippers Evaluation of SSC Pacific.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS

Mamadou H. Diallo
Christopher T. Graves

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC Pacific
53560 Hull Street
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TD 3277

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Advanced Research Projects Agency, Brandeis Program
675 North Randolph Street
Arlington, VA 22203-2114

10. SPONSOR/MONITOR'S ACRONYM(S)

DARPA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

This is work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction.

14. ABSTRACT

This technical document details our teams research of TIPPERS. TIPPERS is a programming platform that provides semantic abstraction for devices, sensors, and virtual sensors to operate in a certain context and obey the policies. TIPPERS is based on earlier research into an Internet of Things (IoT) testbed developed at the University of California, Irvine (UCI), under the DARPA Brandeis program.

15. SUBJECT TERMS

Surveillance; privacy enforcement; policy violation, GPS tracking;

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Mamadou H. Diallo
					19B. TELEPHONE NUMBER *(Include area code)*
U	U	U	U	20	(949)-400-1735

This page is intentionally left blank.

SSC Pacific
San Diego, CA 92152-5001